(12) UK Patent Application (19) GB (11) 2 287 855 (13) A

(43) Date of A Publication 27.09.1995

(21) Application No 9505549.7

(22) Date of Filing 20.03.1995

(30) Priority Data
(31) 9405615 (32) 22.03.1994 (33) GB
9411143 03.06.1994

(71) Applicant(s)
Vodafone Limited

(Incorporated in the United Kingdom)

The Courtyard, 2-4 London Road, NEWBURY, Berkshire, RG13 1JL, United Kingdom

(72) Inventor(s)
Michael Walker
Edward W Beddoes

(74) Agent and/or Address for Service
Mathisen Macara & Co
The Coach House, 6-8 Swakeleys Road, Ickenham, UXBRIDGE, Middlesex, UB10 8BZ, United Kingdom

(51) INT CL[6]
H04M 1/66 , H04Q 7/32

(52) UK CL (Edition N)
H4K KBHG
H4L LDSK L1H10

(56) Documents Cited
EP 0607767 A1 EP 0301740 A2

(58) Field of Search
UK CL (Edition N) H4K KBHG KEM KQJ , H4L LDSK
INT CL[6] H04M , H04Q

(54) Mobile telephone

(57) Mobiles on a GSM cellular telephone system are activated by SIMs (smart cards) which are individually issued to subscribers by service providers. In order to personalise a handset so that it can only be used by SIMs issued by a particular service provider, the service provider can insert a "personalisation control key" (SPCK) which switches an indicator ON in the mobile. Thereafter, the mobile can only be used, in response to insertion of a SIM, if identification data (e.g. the IMSI or International Mobile Subscriber Identity and data identifying the service provider) on the SIM correlates with a stored value. Using this process, a service provider can set each mobile sold to its subscribers so that it can only be activated by SIMs issued by that service provider.

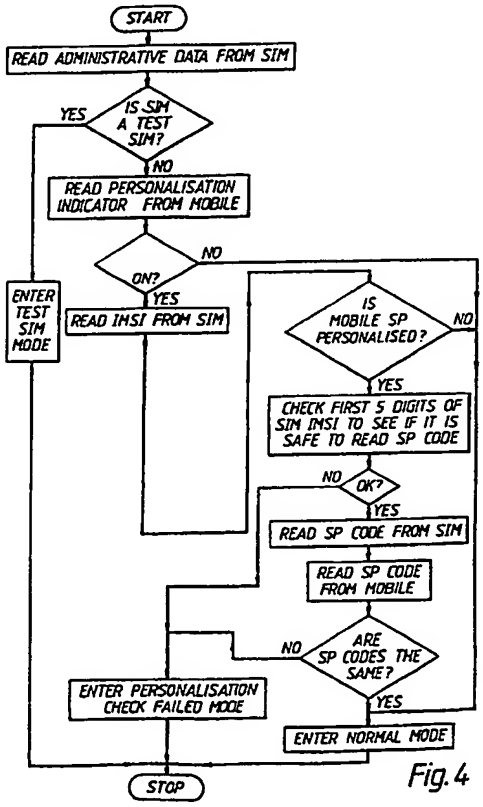

Fig.4

GB 2 287 855 A

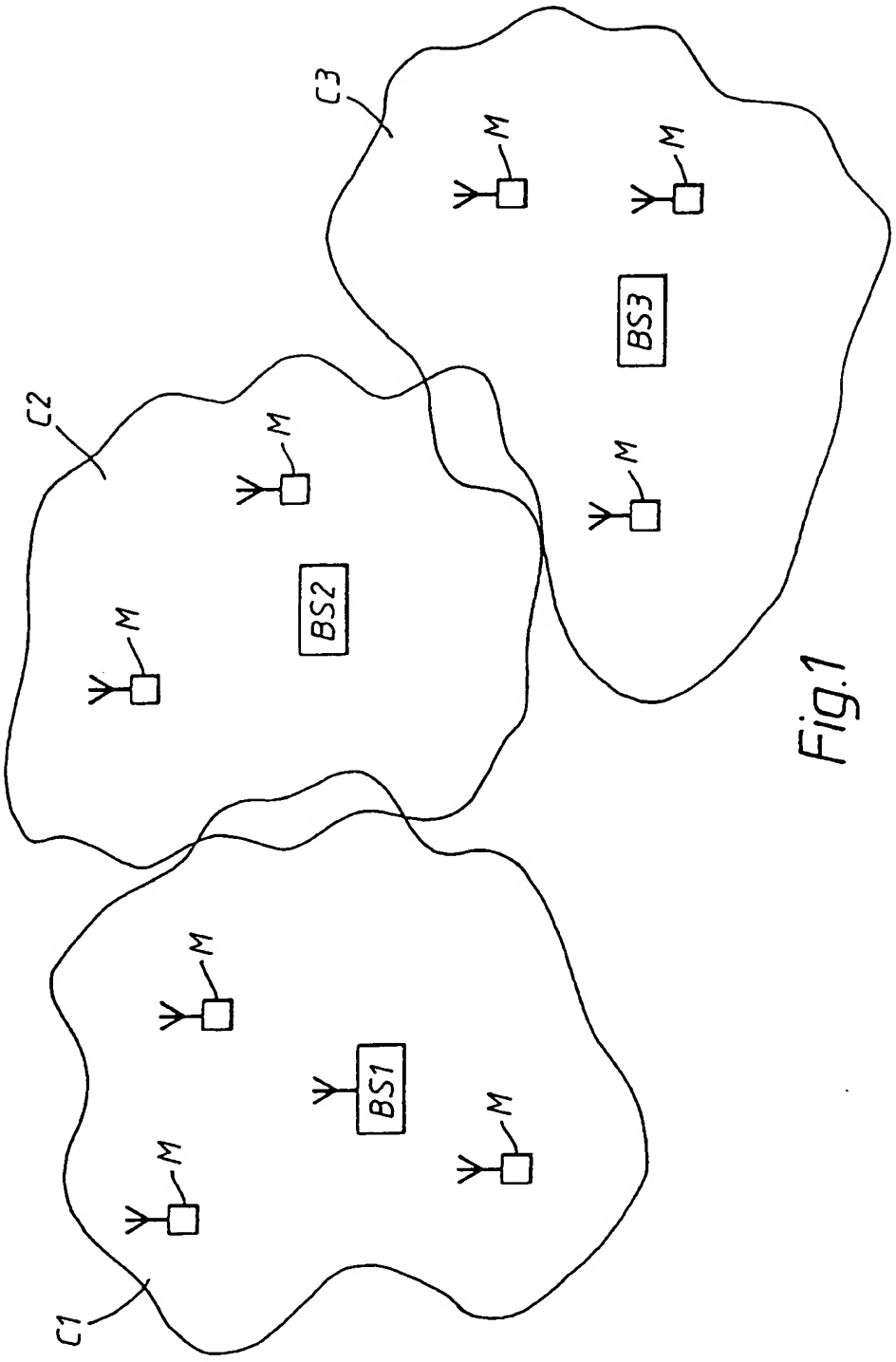

Fig.1

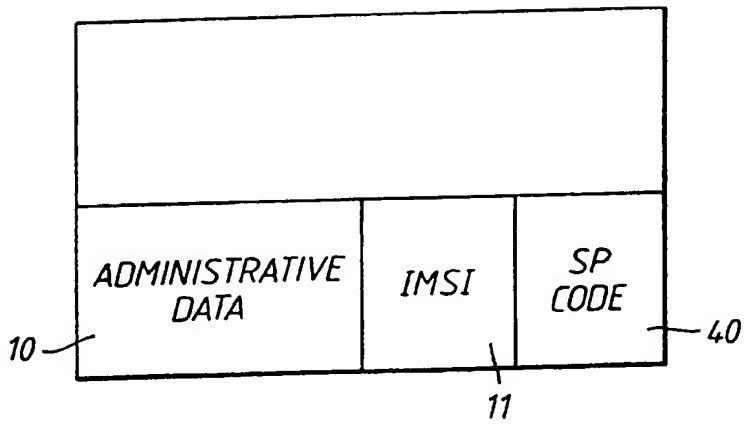

Fig.2

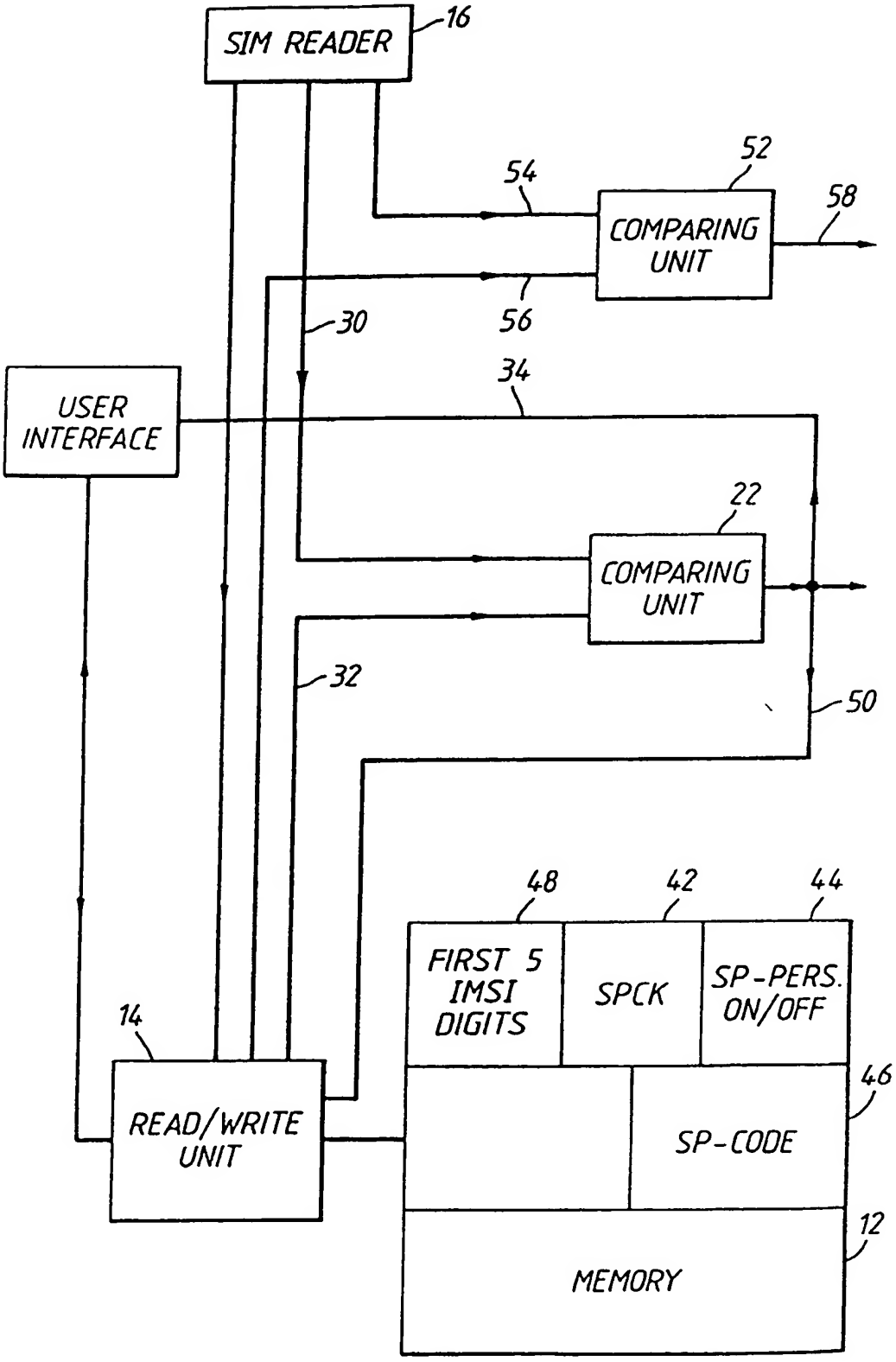
SIM READER
16
52
54
58
COMPARING UNIT
56
30
34
USER INTERFACE
22
COMPARING UNIT
32
50
48
42
44
FIRST 5 IMSI DIGITS
SPCK
SP-PERS. ON/OFF
14
46
READ/WRITE UNIT
SP-CODE
12
MEMORY

Fig.3

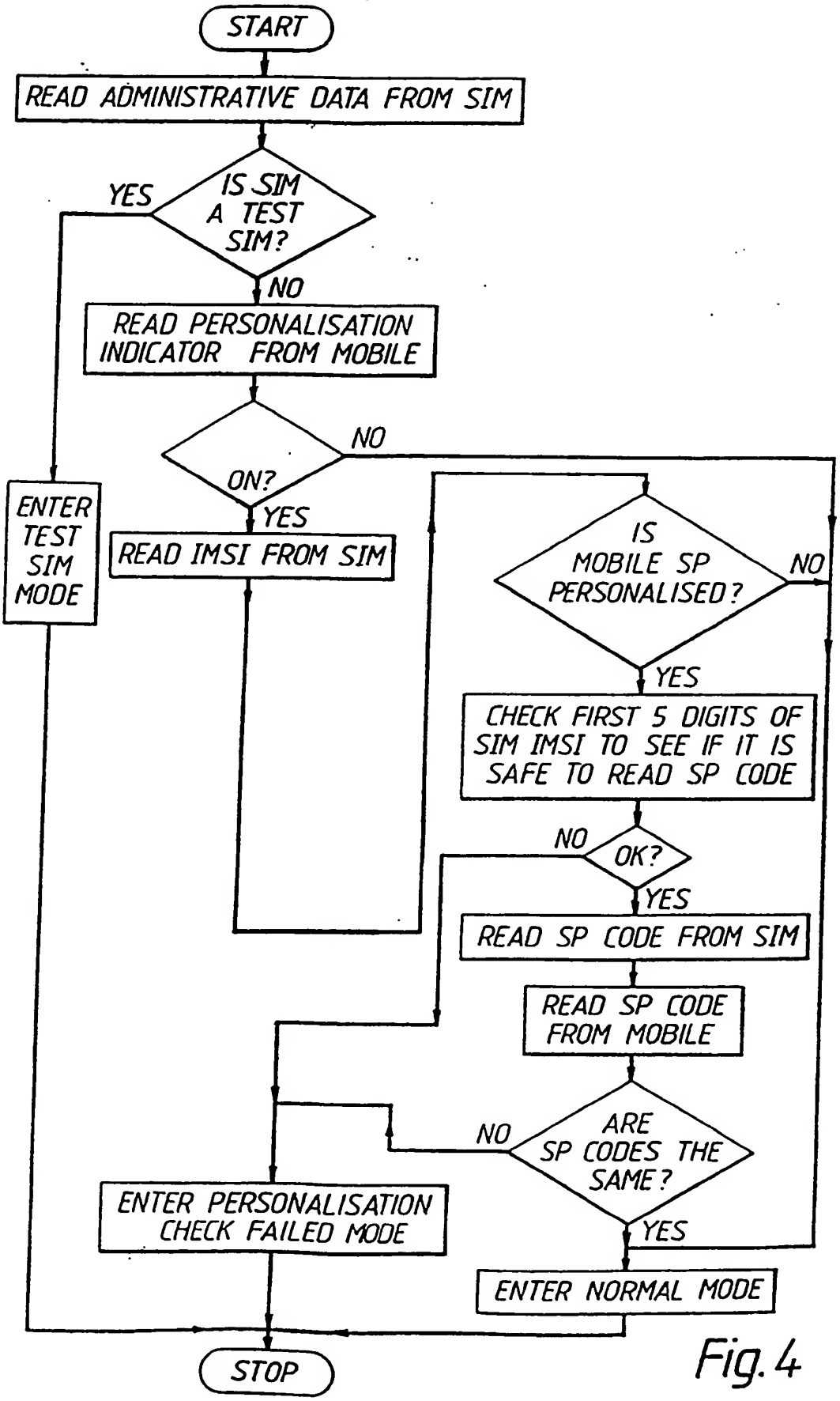
START
READ ADMINISTRATIVE DATA FROM SIM
IS SIM A TEST SIM?
YES
NO
READ PERSONALISATION INDICATOR FROM MOBILE
ON?
NO
YES
ENTER TEST SIM MODE
READ IMSI FROM SIM
IS MOBILE SP PERSONALISED?
NO
YES
CHECK FIRST 5 DIGITS OF SIM IMSI TO SEE IF IT IS SAFE TO READ SP CODE
OK?
NO
YES
READ SP CODE FROM SIM
READ SP CODE FROM MOBILE
ARE SP CODES THE SAME?
NO
YES
ENTER PERSONALISATION CHECK FAILED MODE
ENTER NORMAL MODE
STOP

Fig. 4

TELEPHONE APPARATUS

The invention relates to telephone apparatus. More specifically, the invention relates to telephone handsets for radio telephone systems such as cellular systems. One example of such handset comprises handsets for use in the GSM digital telephone system now in use in European and other countries.

In the GSM system, a user of the system is provided with a token, in the form of a smart card, for activating a handset in the system. Such a smart card is called a Subscriber Interface Module or SIM. A user wishing to use a telephone handset in the system inserts the SIM into the handset. Assuming that various checks which are then carried out produce satisfactory results, the handset is activated and the user can then make and receive calls.

According to the invention, there is provided a telephone handset activatable into a state in which it can make and receive calls by means of a token bearing data identifying the token, comprising control means selectively settable into a restricted condition in which the handset can only be activated by a token having a particular identity, the

particular identity identifying a class of tokens and there being plurality of tokens within that class.

According to the invention, there is further provided a telephone handset for use on a GSM cellular telephone system incorporating a plurality of networks having subscribers each of whom is authorised by a particular one of a plurality of service providers which are each associated with a respective one of the networks, each handset being activatable into a state in which it can make and receive calls via a particular one of the networks by insertion of a smart card ("SIM") bearing data identifying the subscriber and the network with which the service provider authorising the subscriber is associated, and at least some of the SIMs each also bearing data representing an identity code identifying a particular one of a plurality of classes of subscribers, the subscriber identified by each such SIM belonging to the respective class, the handset comprising first control means selectively settable into a first condition in which the handset can only be activated by SIMs bearing that data.

Telephone handsets embodying the invention for use in a GSM cellular telephone system will now be described, by way of

example only, with reference to the accompanying diagrammatic drawings in which:

Figure 1 is a diagram of part of the GSM system;

Figure 2 is a diagram of a SIM for use in one of the handsets;

Figure 3 is a block diagram of one of the handsets; and

Figure 4 is a flow chart illustrating the operations carried out in the handset of Figure 3.

As shown in Figure 1, the GSM system provides radio telephone service within a number of cells C1,C2,C3 etc. which together cover a particular territorial area. Within each cell, a base station BS1,BS2,BS3... provides radio communication between itself and handsets (mobiles or portables) M. The base stations are linked together within the system and will also normally be connected to the public switched telephone network (PSTN). In this way, telephone calls to and from a particular mobile M are routed through the corresponding base station BS which connects the mobile to the other party, perhaps another mobile within the same cell or a fixed telephone, or a mobile

in another cell. In the GSM system, such calls are handled digitally. When a mobile, making or receiving a call, moves into a different cell, a handover process takes place by which the call is transferred to the base station of the next cell. The division of the territorial area into cells enables the frequencies of communication channels to be re-used.

In the GSM system, each subscriber is issued with a Subscriber Identification Module (SIM) in the form of a smart card which is programmed with the subscriber's details and other information. To make or receive a call, the subscriber has to insert the SIM into a GSM handset which then reads the SIM and effectively programs itself to receive calls intended for that subscriber and to make calls which are charged to that subscriber's account.

In principle, therefore, the subscriber may make or receive calls at any GSM handset, because the handset programs itself for that purpose when the subscriber inserts the SIM. It is not therefore necessary for subscribers to have their own telephone handsets; they can use any handset which will respond to insertion of their SIM and can thus receive calls at any such handset (which becomes effectively programmed to

receive telephone calls intended for that subscriber's telephone number) and can make calls from that handset which will be billed to that particular subscriber using the information on the SIM.

It also follows, of course, that if a subscriber owns a telephone handset, it is in principle possible for other subscribers to use the handset (after insertion of their SIMs), without the cost of the calls being charged to the subscriber owning the handset.

However, handsets which can be freely used in response to insertion of any SIM may be liable to theft for that reason. Calls made from such a stolen handset will not be billed to the subscriber owning the handset, but nevertheless the subscriber has lost the handset.

In accordance with a feature of the invention, a handset can be arranged so that it will only function with particular SIMs. In accordance with a feature of the invention, handsets can be programmed or personalised so that they can only be activated by SIMs in a particular class or set. Such a class or set could be defined in any desired way. For example, a

particular service provider, that is, an organisation selling telephone service on a particular network to individual subscribers, can personalise all the handsets which it sells so that they can only be activated by SIMs issued by that particular service provider. In another example, handsets could be personalised so that they can only be activated by SIMs corresponding to a particular class of service.

The operation of this feature will now be described in more detail. It will initially be described with reference to the personalisation of a handset so that it can only be used by SIMs issued by a particular service provider. This is termed "SP-Personalisation". Other variants will also be described.

Figure 2 diagrammatically illustrates a SIM which is preferably in the form of a smart card storing programmable data. As indicated in Figure 2, some of this data, indicated at 10, can be termed administrative data and comprises data identifying the subscriber and other data such as concerned with security. In addition, the SIM stores an International Mobile Subscriber Identity (IMSI). This is a unique number identifying the subscriber and which is thus correlated with (though is not the same as) the subscriber's actual telephone

number. The SIM is also provided with a storage location 40 which stores data representing an identity code, in this case referred to as an "SP code". This comprises data identifying the service provider who has issued the particular SIM.

The SP-Personalisation feature operates by using (in the manner to be described) data which is unique to each SIM.

The IMSI is suitable for this purpose, though other possibilities exist. For example, each SIM may carry a card identification number which could be used, instead of the IMSI, for SP-Personalisation. In what follows, however, it will be assumed that the IMSI is being used for this purpose.

Figure 3 diagrammatically illustrates parts of a handset. As shown, it comprises a memory 12 capable of storing various data which can be written into and read from it by means of a read-write unit 14. The latter is connected to a SIM reader 16 and also to a user interface. The user interface includes the user's keypad and display by means of which the subscriber can input data into the memory 12 and receive information read from it.

The handset also includes a comparing unit 22.

The memory 12 has a storage location 42 storing a "Service Provider Control Key" (SPCK), a storage location 44 storing an SP-Personalisation ON/OFF indicator, and a storage location 46 which stores the SP code of the service provider for whose SIMs the handset is to be personalised. The process for entering the SP code into the memory will be described later.

In the GSM system, the first five digits of all the IMSI's operational in a particular network on the system are the same and thus identify that network (and this distinguish those IMSI's from the IMSI's of other networks also operational on the same GSM system). Each mobile on which the SSP-Personalisationfeature is to be provided therefore has a storage location 48 in its memory 12 which stores the first five digits of the IMSIs of the particular GSM network whose service providers are to have the SP-Personalisation feature.

The SPCK enables the service provider (but not the subscriber) to toggle the SP-Personalisation feature ON and OFF, the SPCK being a code number, similar to a PIN. In order to switch the SP-Personalisation feature between its ON and OFF settings,

the service provider switches the handset into a setting mode (by means not available to the subscriber) and then enters the SPCK by means of the keypad which switches the SSP-Personalisationfrom its present setting to the opposite setting.

It will initially be assumed that the IMSI of the owning subscriber's SIM has been entered into the handset and its first five digits are held in storage location 48. The process for carrying this out will be described later.

The manner in which the handset responds when a SIM is entered into its reader 16 will now be described.

It will also be assumed that a particular service provider's SP code has been entered into the storage location 46 of memory 12, and the operation when a SIM is inserted into the reader 16 will now be described.

Insertion of the SIM activates the read/write unit 14 to address the storage location 44 in order to check whether the SP-Personalisation indicator is ON or OFF. If the indicator is OFF, the mobile then automatically enters the normal mode

for receiving or making calls.

If the SP-Personalisation indicator in storage location 44 is ON, however, the IMSI is read from the SIM by the reader 16 and passed to the comparison unit 22. At the same time, the first five IMSI digits are read out of the storage location 48 by the read/write unit 14 and passed to the comparison unit 22.

If the comparing unit 22 determines that the first five digits of the IMSI in the currently read SIM are not correct, thus indicating that the SIM is not operational on the particular network identified by those digits, it causes the handset to enter the "personalisation check failed" mode and further use is blocked (until a correct SIM is inserted or until the SSP-Personalisationfeature is toggled OFF by the service provider). If the comparison carried out by the comparing unit 22 is successful, it produces an output on a line 50 which causes the reader 16 to read out the SP code from the storage location 40 of the SIM (see Figure 2) and to pass it to a further comparing unit 52 on a line 54. At the same time, the read/write unit 14 is activated to feed out the stored SP code from storage location 46 and to feed it to the

comparing unit 52 on a line 56. The two SP codes are then compared. If they are found to be the same, the comparing unit 52 produces an output on a line 58 which causes the mobile to enter the normal mode for receiving and making calls. If the two SP codes are not the same, the mobile enters a "personalisation check failed" mode and further use is blocked (until a correct SIM is inserted or until the SSP-Personalisationfeature is toggled OFF by the service provider).

The purpose of the comparing unit 22, and the initial check of the first five digits of the IMSI, is to ensure that the reader 16 does not interrogate the SIM for the SP code until it has first determined (by inspecting the first five digits of the IMSI of that SIM) that the SIM has in fact been issued by the appropriate network. This feature is provided in order to prevent possible misinterpretation of data on a SIM issued by a service provider of another network.

A mobile may incorporate other security features in addition to the SP-Personalisation feature described. Thus, the mobile may additionally be arranged so that it can only be activated by a particular subscriber's SIM. Such a feature can be

capable of being toggled ON or OFF. Therefore, if it is toggled OFF, another subscriber's SIM can be used to activate the mobile, but only subject to the SP-Personalisation feature described above. If the SP-Personalisation feature is ON, that other subscriber must be a subscriber of the relevant service provider. If the subscriber is not a subscriber of that service provider, then they will not be able to use the handset unless the SP-Personalisation feature is toggled OFF (by the service provider).

Figure 4 is a flow chart illustrating the process of carrying out the SP-Personalisation checks on the mobile. The system may be arranged to be responsive to special "test" SIMs for carrying out certain functional tests on the handset. As shown in Figure 4, there is therefore a first stage in the operations carried out which comprises checking whether or not the SIM is a test SIM. If it is found to be a test SIM, the handset enters a special test mode.

As so far described, the identity of a SIM is checked explicitly for correctness - that is, an identification is read from the SIM and compared with a pre-stored identity in the mobile. Instead, however, the identity of a SIM can be

checked implicitly. For example, the mobile could apply a predetermined interrogation or challenge to an inserted SIM and check the SIM's response by comparing it against a predetermined value for such response stored in the mobile.

Setting up of the SP-Personalisation feature is carried out by a supervising authority which would normally be the service provider.

In order to set up the SP-Personalisation feature initially, the Service Provider inserts a SIM and selects an SSP-Personalisationoption from a suitable menu (which is not available to the normal subscriber). The mobile then reads the IMSI from the SIM and stores the value of its first five digits. These first five digits identify the network with which the Service Provider is associated. Their storage enables a check to be made on subsequently inserted SIMs to ensure that they are appropriate to the correct network (that is, the network with which the Service Provider is associated). In other words, the purpose of storing these first five digits is to avoid the need for the SP code to include data identifying the correct network.

The mobile then reads the SP code from the SIM (from its storage location 40, see Figure 2) and stores it in the storage location 46 (Fig. 2), overwriting any existing value.

The Service Provider is then prompted to choose and enter the SPCK which becomes stored in the storage location 42 (Figure 3), overwriting any existing value. The SP-Personalisation indicator (storage location 44) becomes set to ON.

The SP-Personalisation indicator then remains ON until it is switched to OFF by the Service Provider. This is carried out by the Service Provider selecting a de-personalisation option and then inserting the correct SPCK. Under certain circumstances, a subscriber might be permitted to toggle the SP-Personalisation ON and OFF.

The above process, for setting up the SP-Personalisation feature can only be carried out if the SP-Personalisation indicator is currently set to OFF.

The SP code and any part of the IMSI needed to identify the network (the first five digits in the example given above)

need not be entered via the SIM but could be initially entered by other means.

The SP-Personalisation feature may be set up on behalf of the administrator of the range or class of SIMs to which it applies by some other party who may have programmed the SP code and that part of the IMSI which identifies the network operator directly to the handset. Such other party might be a manufacturer, for example.

The mobiles may be arranged so that they can be unpersonalised (that is, the SP-Personalisation feature can be switched OFF) without use of the SPCK. This facility may be required for the case where the Service Provider has forgotten the appropriate key, if the mobile has been sold without being de-personalised, or if it is returned for repair without having been de-personalised and without the appropriate SIM. Any such de-personalisation should be available only under security-controlled conditions - for example, key or password control.

Although the foregoing description of the feature of the invention by which handsets can be programmed so that they can

only be operated by a particular range or class of SIMs has used the example where the SIMs are those issued by a particular service provider, it will be understood that the range or class of the SIMs can be defined in any other desired way.

For example, the range or class of SIMs could be those issued to persons belonging to or employed by a particular company or other organisation or association or its customers or members. In other words, only those SIMs would be able to activate the mobile if the personalisation feature (generically termed "corporate-personalisation") is ON. Corporate-personalisation would be implemented generally in the manner described above. It would be toggled ON or OFF by means of a "corporate control key" CCK stored in storage location 42 (Figure 3), which would perform the same function as the SPCK referred to above. The storage location 46 (Figure 3) would in this case store a "corporate provider" code (CP), that is, a code identifying the particular company or organisation.

Another possibility is for the range or class of SIMs capable of activating the mobile to be those particular to only one network provider. This for example prevents the export of

stolen mobiles to other countries. The operation is again generally the same as described above. The SPCK or CCK in storage location 42 (Figure 3) would be replaced by a "network control key" (NCK) and the SP or CP code in storage location 46 would be replaced by a network provider code (NP).

Corporate-personalisation or network personalisation would be set up in generally the same way as described above for SSP-Personalisation The setting up of corporate-personalisation could be restricted to the service provider. Instead, the company or other organisation might be permitted to carry it out themselves. The setting up of the network personalisation feature would normally be restricted to the service provider.

The ranges or classes of SIMs capable of permitting operation of a handset can of course be defined in other ways than those described above.

CLAIMS

1. A telephone handset activatable into a state in which it can make and receive calls by means of a token bearing data identifying the token, comprising control means selectively settable into a restricted condition in which the handset can only be activated by a token having a particular identity, the particular identity identifying a class of tokens and there being plurality of tokens within that class.

2. A handset according to claim 1, in which the control means is selectively settable out of the restricted condition so that the handset can be activated by tokens not having that particular identity.

3. A handset according claim 1 or 2, in which each token is a smart card.

4. A handset according to any preceding claim, in which the handset is a GSM handset.

5. A handset according to any preceding claim, in which the control means comprises storage means for storing data representing the particular identity, reading means for

reading from a token the data identifying the token, and comparing means operative to compare the stored data and the read data and operative to determine whether the token has the said particular identity.

6. A handset according to any one of claims 1 to 4, in which the control means comprises interrogation means for interrogating the token in a predetermined manner so that the token produces a response dependent on its identity, storage means for storing data representing the response dependent on the particular identity, and comparing means operative to compare the produced response with the stored data and operative to determine whether the token has the said particular identity.

7. A handset according to any preceding claim, in which the control means includes storage means for storing indicating data indicating whether the control means is or is not in the said restricted condition.

8. A handset according to any preceding claim, including setting means for setting the control means into and out of the said restricted condition, the setting means being

operable by means of a key.

9. A telephone handset for use on a GSM cellular telephone system incorporating a plurality of networks having subscribers each of whom is authorised by a particular one of a plurality of service providers which are each associated with a respective one of the networks, each handset being activatable into a state in which it can make and receive calls via a particular one of the networks by insertion of a smart card ("SIM") bearing data identifying the subscriber and the network with which the service provider authorising the subscriber is associated, and at least some of the SIMs each also bearing data representing an identity code identifying a particular one of a plurality of classes of subscribers, the subscriber identified by each such SIM belonging to the respective class, the handset comprising first control means selectively settable into a first condition in which the handset can only be activated by SIMs bearing that data.

10. A handset according to claim 9, in which the said data representing the identity code is stored in first storage means of the SIMs, and in which the first control means comprises second storage means for storing data representing

that identity code and comparing means operative in response to insertion of a SIM to compare the identity code stored in the first storage means of the SIM with the data in the second storage means and operative to control the activation of the handset in dependence on the results of the comparison.

11. A handset according to claim 10, in which all those SIMs bearing the identity code identifying a particular class of subscribers bear data identifying the same network, and in which the second storage means also stores data identifying the network respective to the identity code which it stores.

12. A handset according to claim 11, in which the first control means is inhibited unless the data stored on the SIM identifying the network identifies that network as being the same network as the network identified by the data in the second storage means.

13. A handset according to any one of claims 9 to 12, including means responsive to data input into the first control means by a supervising authority for switching the handset into and out of the said first condition.

14. A handset according to claim 13, in which the supervising authority is a particular service provider.

15. A handset according to any one of claims 9 to 14, in which the data stored on the SIM and identifying the particular subscriber comprises the subscriber's International Mobile Subscriber Identity (IMSI).

16. A handset according to claim 12, in which the data stored on the SIM and identifying the particular subscriber comprises the subscriber's International Mobile Subscriber Identity (IMSI), and in which the data stored on each SIM identifying the network with which the service provider authorising the subscriber respective to that SIM is associated comprises a predetermined part of the IMSI.

17. A handset according to any one of claims 9 to 16, in which each of the plurality of classes of subscribers comprises the subscribers authorised by a particular service provider.

18. A handset according to any one of claims 9 to 16, in which each of the plurality of classes of subscribers

comprises subscribers employed by, belonging to, members of or authorised by a particular company or organisation.

19. A handset according to any one of claims 9 to 16, in which each of the plurality of classes of subscribers comprises subscribers authorised by service providers associated with a particular network.

20. A smart card for a handset according to any one of claims 9 to 19, including a storage location for storing data identifying a particular one of the said service providers.

21. In combination, a telephone handset and a smart card (SIM) substantially as described with reference to Figures 2 and 3 of the accompanying drawings.

22. In combination, a telephone handset and a smart card (SIM) substantially as described with reference to Figures 2 to 4 of the accompanying drawings.

Patents Act 1977 Examiner's report to the Comptroller under Section 17 (The Search report)	Application number GB 9505549.7
Relevant Technical Fields (i) UK Cl (Ed.N) H4K: KBHG; KEM; KQJ. H4L: LDSK (ii) Int Cl (Ed.6) H04M, H04Q	Search Examiner AL STRAYTON Date of completion of Search 16 MAY 1995
Databases (see below) (i) UK Patent Office collections of GB, EP, WO and US patent specifications. (ii)	Documents considered relevant following a search in respect of Claims :- ALL

Categories of documents

X:	Document indicating lack of novelty or of inventive step.	**P:**	Document published on or after the declared priority date but before the filing date of the present application.
Y:	Document indicating lack of inventive step if combined with one or more other documents of the same category.	**E:**	Patent document published on or after, but with priority date earlier than, the filing date of the present application.
A:	Document indicating technological background and/or state of the art.	**&:**	Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages		Relevant to claim(s)
A	EP 0607767 A1	(ERICSSON)	
A	EP 0301740 A2	(NOKIA)	

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).